AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on line 24 of page 13 with the following amended paragraph:

In an aspect of the present invention, an AES encryption processor is composed of a selector unit selecting an element of a state in response to row and column indices, a S-box for obtaining a substitution value with the selected element used as an index, a coefficient table providing first to fourth coefficients in response to the row index, first to fourth ~~Galois field multiplexers~~Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state.

Please replace the paragraph beginning on line 23 of page 14 with the following amended paragraph:

In another aspect of the present invention, an AES encryption processor is provided which is adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state. The AES encryption processor is composed of a selector unit selecting an element of the state in response to the first operand and the immediate operand, the selected element being stored in the input register, a S-box for obtaining a substitution value with the selected element used as an index, a coefficient table providing first to fourth coefficients in response to the immediate operand, first to fourth ~~Galois field multiplexers~~Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and a storing unit for storing the first to fourth products into the output register selected by the second operand.

Please replace the paragraph beginning on line 25 of page 15 with the following amended paragraph:

In still another aspect of the present invention, an AES decryption processor is composed of a selector unit selecting an element of a state in response to row and column indices, an inverse S-box for obtaining a substitution value with the selected element used as an index, a coefficient table providing first to fourth coefficients in response to the row index, first to fourth ~~Galois field multiplexers~~Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state.

Please replace the paragraph beginning on line 14 of page 16 with the following amended paragraph:

In still another aspect of a present invention, an AES decryption processor is provided which is adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state. The AES decryption processor is composed of a selector unit selecting an element of the state in response to the first operand and the immediate operand, the selected element being stored in the input register, a S-box for obtaining a substitution value with the selected element used as an index, a coefficient table providing first to fourth coefficients in response to the immediate operand, first to fourth ~~Galois field multiplexers~~Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and a storing unit for storing the first to fourth products into the output register selected by the second operand.

Please replace the paragraph beginning on line 9 of page 8 with the following amended paragraph:

In still another aspect of the present invention, an AES processor adapted to both encryption and decryption is composed of a first selector unit selecting an element of a state in response to row and column indices, an inverse affine transformation circuit applying an inverse affine transformation on the selected element, a second selector unit selecting one out of two data bytes consisting of the selected element received from the first selector, and a result of the inverse affine transformation received the inverse affine transformation circuit, wherein the selected element is selected for encryption, while the result of the inverse affine transformation is selected for decryption, an inverse determining unit obtaining a multiplicative inverse of the selected data byte received from the second selector, an affine transformation circuit applying an affine transformation on the obtained multiplicative inverse, a third selector unit selecting one of two data bytes consisting of the multiplicative inverse received from the inverse determining unit, and a result of the affine transformation received from affine transformation circuit, wherein the result of the affine transformation is selected for decryption, while the multiplicative inverse is selected for encryption, a coefficient table providing first to fourth coefficients in response to the row index, first to fourth ~~Galois field multiplexers~~ Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state.

Please replace the paragraph beginning on line 20 of page 18 with the following amended paragraph:

In still another aspect of the present invention, an AES processor is provided which is adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state. The AES processor is composed of a first selector unit selecting an element of the state in response the first operand and the immediate operand,

the selected element being stored in the input register, an inverse affine transformation circuit applying an inverse affine transformation on the selected element, a second selector unit selecting one out of two data bytes consisting of the selected element received from the first selector, and a result of the inverse affine transformation received the inverse affine transformation circuit, wherein the selected element is selected for encryption, while the result of the inverse affine transformation is selected for decryption, an inverse determining unit obtaining a multiplicative inverse of the selected data byte received from the second selector, an affine transformation circuit applying an affine transformation on the obtained multiplicative inverse, a third selector unit selecting one of two data bytes consisting of the multiplicative inverse received from the inverse determining unit, and a result of the affine transformation received from affine transformation circuit, wherein the result of the affine transformation is selected for decryption, while the multiplicative inverse is selected for encryption, a coefficient table providing first to fourth coefficients in response to the row index, first to fourth ~~Galois field multiplexers~~ Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and a storing unit for storing the first to fourth products into the output register selected by the second operand.

Please replace the paragraph beginning on line 9 of page 20 with the following amended paragraph:

In still another aspect of the present invention, an AES processor is provided which is adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state(s). The AES processor is composed of a plurality of AES processor cores respectively associated with a plurality of columns of the state(s), a coefficient table providing first to fourth coefficients in response to the immediate operand. Each of the plurality of AES processor cores includes a first selector unit selecting an element of the state(s) in response the first operand and the immediate operand, the selected element being stored in the input register, an inverse affine transformation circuit applying an inverse affine transformation on the selected

element, a second selector unit selecting one out of two data bytes consisting of the selected element received from the first selector, and a result of the inverse affine transformation received the inverse affine transformation circuit, wherein the selected element is selected for encryption, while the result of the inverse affine transformation is selected for decryption, an inverse determining unit obtaining a multiplicative inverse of the selected data byte received from the second selector, an affine transformation circuit applying an affine transformation on the obtained multiplicative inverse, a third selector unit selecting one of two data bytes consisting of the multiplicative inverse received from the inverse determining unit, and a result of the affine transformation received from affine transformation circuit, wherein the result of the affine transformation is selected for decryption, while the multiplicative inverse is selected for encryption, first to fourth ~~Galois field multiplexers~~ Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and a storing unit for storing the first to fourth products into the output register selected by the second operand.

Please replace the paragraph beginning on line 9 of page 40 with the following amended paragraph:

The ~~Galois field multiplexers~~ Galois field multipliers 107_0 to 107_3 respectively receive the coefficients d_0 to d_3 from the auxiliary register 406, and compute the produces of the selected byte (or element) with the corresponding coefficients. The computed products constitute resultant four-byte data, and the four-byte data is stored in the result register 408. The four-byte data stored in the result register 408 is selected by the write multiplexer 412 and transferred to the output register rt, which is selected from among the registers within the register file 401 by the operand rt received from the decoder 403.

Please replace the paragraph beginning on line 3 of page 46 with the following amended paragraph:

Referring to Fig. 16, the AES processor in this embodiment includes an inverse affine transformation circuit 1101, an encryption multiplexer 1102, an inverse table 1103, an affine transformation circuit 1104, an encryption multiplexer 1105, a row multiplexer 104, a coefficient table 106, ~~Galois field multiplexers~~ Galois field multipliers 107, and a result register 108.